THE TROUBLE WITH TRESPASS*

by
Dan L. Burk**

Courts wrestling with disputes about access to computer networks have embraced an archaic cause of action: trespass to chattels. Unfortunately, the courts had to mangle the traditional elements of the action to allow the facts of the cases to fit into the legal box. Courts have found damage to the chattel, for example, in the cost of resisting access. The analysis used in the Internet trespass to chattels cases potentially describes every access to all digital media. In lieu of the common law trespass to chattels cause of action, the author proposes a new theory of digital nuisance as a mechanism for balancing competing interests.

I. INTRODUCTION.....	27
II. TRESPASS IN THE COURTS.....	28
III. TRESPASS IN THE LAW	32
A. Intermeddling	32
B. Impairment	34
C. Consent.....	37
IV. TRESPASS IN CYBERSPACE	39
A. Copyright's Cousin	40
B. Trespass to Web Sites	43
C. Incomplete Entitlements	47
V. CONCLUSION	54

I. INTRODUCTION

This Essay is about trespass, specifically about trespass to chattels, which seems to have become the darling of cyberspace lawyers. In a series of recent decisions, led by the opinion in *CompuServe v. Cyber Promotions*,¹

* Copyright 1999 by Dan L. Burk.

** Visiting Professor of Law, University of Minnesota. This Essay was presented at the Fifth Annual Lewis & Clark Law Forum, *Intellectual Property in the New Millennium: Keeping Pace with Change*, October 1, 1999. I thank the organizers of the Forum, particularly Prof. Lydia Loren, for the opportunity to develop the ideas presented here, and Ms. Arlene Forrest for her capable research assistance.

¹ *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997).

courts have used this obscure nineteenth century claim² to exclude unsolicited bulk e-mail or "spam"³ first from the computer systems of Internet subscription services, and more recently from corporate computer systems. An exposition upon bulk e-mail and trespass to chattels might seem out of place in a symposium devoted to the "Intellectual Property in the Next Millennium." But the law of intellectual property never deals absolutely with intangible interests; rather, it coalesces about their tangible embodiment.⁴ In this Essay I shall argue that the bulk e-mail cases I have mentioned recognize a novel proprietary interest for which the label "trespass to chattels" is merely a convenient apology. Indeed, I suggest that what we are now observing in the context of the Internet is not only a new form of proprietary interest, but no less than the emergence of a new form of intellectual property, with only the most tenuous of antecedents in the law of chattels. I shall further show that the form the courts have given to this new possessory right is fraught with unintended and undesirable consequences. I shall begin by reviewing and critiquing the cases that have given birth to cyberspace trespass actions, then shall indicate the ramifications of such actions, showing why they are particularly ill-suited to a medium that draws its unique benefits from shared resources. I conclude with some suggestions as to how the courts might fashion causes of action that could serve equally well to exclude inappropriate bulk e-mail, but which are more appropriate to networked media.

II. TRESPASS IN THE COURTS TRESPASS IN THE COURTS

Trespass to chattels is a somewhat obscure tort action arising out of unauthorized dispossession, use, or interference with the tangible property of another.⁵ Under the Restatement formulation, the trespass action requires some intentional physical contact with the chattel.⁶ Unlike its cousin, trespass to land, trespass to chattel requires some substantial interference with the chattel, such as removal, damage, or similar impairment of its physical condition.⁷ Trivial interferences never constitute a dispossession, but the harm necessary to trigger liability may arise from an injury to someone or something other than the chattel itself, so long as the harm bears a proximate relationship to the dispossession.⁸

One could easily envision the application of this tort claim to a variety of computer-related situations in which unauthorized users impaired

² See DAN B. DOBBS, *THE LAW OF TORTS* § 60 (2000) (tracing the historical roots of trespass to chattels from actions in detinue and trover).

³ See *WIREDSTYLE: PRINCIPLES OF ENGLISH USAGE IN A DIGITAL AGE* 78 (Constance Hale ed., 1996) (defining "spam"); ANDY IHNATKO, *CYBERSPEAK* 179 (1997) (defining "spam").

⁴ See, e.g., 17 U.S.C. § 101 (1994).

⁵ See *RESTATEMENT (SECOND) OF TORTS* §§ 217-218 (1965).

⁶ *Id.* § 217 cmt. e.

⁷ *Id.* §§ 218, 221; DOBBS, *supra* note 2, at 124.

⁸ See DOBBS, *supra* note 2, at 124-25.

the function of a computer system, perhaps by damaging hardware or software, or even by locking the owner out of important computer files.⁹ But the theory has in fact been applied in somewhat more exotic settings, where its suitability is more dubious. Trespass to chattels debuted in this context in a California Court of Appeals case, *Thrifty-Tel v. Bezenek*¹⁰ involving an intrusion on the equipment of a telephone services provider. In *Thrifty-Tel*, a long-distance telephone provider brought an action for conversion against parents whose minor children had been engaged in what more sophisticated hackers might term "phreaking": the unauthorized use of telephone services.¹¹ The children had initially gained access to the Thrifty-Tel system by manually entering randomly guessed telephone authorization codes; later they acquired and employed software to conduct high-speed automated searches for access codes.¹²

Although the telephone provider sued for damages under a theory of conversion, the court on appeal substituted its own theory of trespass to chattels.¹³ The court acknowledged that conversion generally requires appropriation of some tangible article, and it was unclear whether telephone access codes or telephone services could be converted.¹⁴ But the court concluded without any serious analysis that an unauthorized use of a telephone system could constitute trespass to chattels.¹⁵ In a footnote, the court concluded that the electronic signals generated by the children were "sufficiently tangible to support a trespass cause of action."¹⁶ In support of this conclusion, the court cited several cases holding that dust or sound waves could constitute trespass if they caused damage, rather than simply interfering with the use or enjoyment of property.¹⁷

The *Thrifty-Tel* decision paved the way for subsequent application of trespass to chattels to computer networks. The leading opinion has been that of the trial court in an action by a proprietary network system, CompuServe, against Cyber Promotions, a commercial service that transmitted unsolicited bulk e-mail, colloquially known as "spam," to thousands of user addresses on the CompuServe network.¹⁸ CompuServe alleged that its subscribers had complained about receiving such transmissions, and some had cancelled their subscription to the service in protest.¹⁹ Com-

⁹ Cf. *State v. Moran*, 784 P.2d 730, 732 (Ariz. Ct. App. 1989) (employee who refused to decode files criminally charged with "recklessly . . . tampering with the property of another person so as substantially to impair its function or value.").

¹⁰ *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).

¹¹ See *WIREDSTYLE*, *supra* note 3, at 76; *IHNATKO*, *supra* note 3, at 150-51.

¹² *Thrifty-Tel*, 54 Cal. Rptr. 2d at 471.

¹³ *Id.* at 472-73.

¹⁴ *Id.* at 472.

¹⁵ *Id.* at 473.

¹⁶ *Id.* at 473 n.6.

¹⁷ *Id.*

¹⁸ *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997).

¹⁹ *Id.* at 1023.

puServe introduced evidence that it had deployed software filters in an attempt to screen out e-mail from Cyber Promotions, but that the bulk e-mailer had evaded the filters by changing or falsifying the originating domain in its message headers.²⁰ CompuServe had also notified Cyber Promotions's owner, Sanford Wallace, that its e-mail transmissions were unwelcome on the CompuServe system.²¹

When such self-help measures were unavailing, CompuServe successfully sought to enjoin the spam on a theory of trespass to chattels. Relying on *Thrifty-Tel*, the Ohio court found that the electronic signals received by the CompuServe system were sufficiently tangible to support a trespass claim.²² The court further found that the contact was intentional, because the e-mail was affirmatively directed to CompuServe e-mail addresses.²³ Although the court agreed with the defendant that the transmissions of the messages over the CompuServe system did not amount to a dispossession of the system, it held the plaintiffs did not need to show physical dispossession to maintain a trespass action.²⁴ Rather, it held that the Restatement test only required the owner to show an interference that impaired the value of the chattel, and not necessarily impairment of the chattel's physical condition.²⁵ The court found that CompuServe showed impairment by demonstrating that the spam was a burden on CompuServe's equipment—processing spam consumes computer processing cycles and occupies computer memory space.²⁶ Alternatively, the court found that CompuServe was adversely affected by the loss of employee time and resources devoted to attempts to block e-mail from Cyber Promotions.²⁷ Finally, the court found harm to the subscriber goodwill associated with CompuServe's services.²⁸

In response to the defendant's argument that its transmissions were permissible once CompuServe had connected its system to the greater Internet, the court recognized some tacit consent to the transmission of e-mail over its system.²⁹ However, the court reasoned that consent did not extend to bulk e-mail transmissions.³⁰ The terms of use for CompuServe facilities excluded unsolicited e-mail, as stated in a policy statement posted online.³¹ CompuServe also expressly revoked any implied invitation to use its facilities by notifying Cyber Promotions that it was prohib-

²⁰ *Id.* at 1019.

²¹ *Id.* at 1024.

²² *Id.* at 1021.

²³ *Id.*

²⁴ *Id.* at 1021-22.

²⁵ *Id.* at 1022.

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.* at 1023.

²⁹ *Id.*

³⁰ *Id.* at 1024.

³¹ *Id.*

ited from sending further junk e-mail to CompuServe addresses.³² The court drew analogies to business owners revoking a general invitation to the public to enter their premises³³ and to property owners demanding that newspaper distributors cease throwing unsolicited newspapers onto their property.³⁴

The reasoning of *CompuServe* has since been adopted wholesale without additional analysis in several suits by other Internet service providers seeking to enjoin spam.³⁵ For the most part, these suits presented factual profiles identical to that in *CompuServe*. However, a new dimension was added to e-mail trespass in the context of a legal dispute between Intel Corporation and a former employee, Kenneth Hamidi.³⁶ Intel successfully enjoined transmission of non-commercial e-mail messages to its computers by Hamidi, who had previously left the firm due to a dispute over a work-related injury.³⁷ Although previously a model of employee loyalty, he became disaffected and bitter toward the computer chip manufacturer, spearheading an anti-Intel information campaign under the auspices of FACE-Intel (Former and Current Employees of Intel).³⁸ Hamidi maintains a FACE-Intel web site containing articles and testimonials about his former employer's purported misdeeds.³⁹ Much of the material on the site is directed to prospective employees of Intel, including college students, warning them against accepting an offer from the company. Other materials on the site are directed to current Intel employees, encouraging them to leave or to demand that the company mend its ways.⁴⁰

Prior to the injunction, Hamidi also directed an e-mail campaign toward current Intel employees, sending them information and admonitions similar to those on his web site, including calls to action, unsavory stories about the company, and details of Hamidi's own dispute against the company.⁴¹ Over a three-year period, Hamidi appears to have sent such bulk e-mail messages on seven different occasions, targeting several thousand recipients at a time.⁴² Hamidi alleges that he obtained the

³² *Id.*

³³ *Id.*

³⁴ *Id.* at 1027.

³⁵ See, e.g., *America Online v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998); *America Online v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998).

³⁶ See *Intel Corp. v. Hamidi*, No. 98AS05067, 1999 WL 450944 (Cal. App. Dep't Super. Ct. Apr. 28, 1999).

³⁷ *Id.* at *3.

³⁸ See Jonathan Rabinovitz, *Gadfly Presses His E-mail Case Against Intel Corp.*, SAN JOSE MERCURY NEWS, July 6, 1999 (page not available).

³⁹ See *Intel Says Spamming is Trespass*, WIRED NEWS (Apr. 28, 1999) <<http://www.wired.com/news/politics/0,1283,19395,00.htm>>.

⁴⁰ See generally *FACE Intel* (visited Feb. 20, 2000) <<http://www.faceintel.com>>.

⁴¹ See *Intel Says Spamming is Trespass*, *supra* note 39.

⁴² See Maria Alicia Guara, *E-Mail Delivered by Horse-Mail; Intel Gadfly Carries on His Vendetta the Old-Fashioned Way*, S.F. CHRON., Sept. 29, 1999, at B2.

employees' e-mail addresses from publicly available Internet sources,⁴³ and that he has a right of public access to the Intel system for purposes of disseminating his message.⁴⁴ Intel, however, alleged that Hamidi's e-mail was an unprivileged use of their private system, and it sent letters to Hamidi demanding that he stop sending the e-mails. When Hamidi persisted in spite of the demand, and despite attempts to filter his messages out, Intel obtained an injunction on a theory of trespass to chattels drawn from the commercial spam cases. As in the case of CompuServe, Intel claimed that once it notified Hamidi that his messages were unwelcome, further transmissions constituted an interference with their system. Unlike CompuServe, Intel could not claim that it lost customers from the transmission, since it is not in the business of providing Internet access. But it could claim that the company was injured due to the time and effort spent attempting to block the messages. Hamidi has continued to deliver his messages, but now does so on paper to Intel's gate, traveling by horse and carriage to emphasize what he believes are the luddite tendencies of the injunction.⁴⁵

III. TRESPASS IN THE LAW

Ken Hamidi's creative method of continuing to deliver his message invites a closer consideration of suitability of a common law claim developed in physical space when applied to the Internet. Hamidi's case further suggests that the claim of "trespass" is mutating from an innovative claim to deter commercial spam into a more general claim to deter unwanted messages. This change has troubling implications for the free flow of information on the network, but it is all the more troubling when the cyberspace application of the claim is closely analyzed against the requirements of the common law action.

A. *Intermeddling*

The incongruity between common law trespass to chattels and the problem of spam is immediately apparent by taking a careful look at the requirement of dispossession or similar interference. Because trespass to chattels requires some type of physical interference with the chattel,⁴⁶ the *CompuServe* opinion finds this physical contact in the passage of electrons over the service provider's system.⁴⁷ To reach this conclusion, the court in *CompuServe* relied heavily on the only available precedent, *Thrifty-Tel*.⁴⁸

⁴³ See Appellant's Brief, *Intel Corp. v. Hamidi*, No. 98AS05067, 1999 WL 450944 (Cal. App. Dep't Super. Ct. Apr. 28, 1999), available at <<http://www.intelhamidi.com/appealbrief.htm#2>> (brief filed by Kenneth Hamidi).

⁴⁴ Rabinowitz, *supra* note 38.

⁴⁵ See Guara, *supra* note 42.

⁴⁶ See RESTATEMENT (SECOND) OF TORTS §§ 217, 218 (1965).

⁴⁷ *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997).

⁴⁸ *Id.* at 1021-22.

The *Thrifty-Tel* opinion, in turn, analogized the passage of electrons over a telephone system to the impact of "intangible" particles.⁴⁹ Speaking specifically of the requirement of a physical touching of the chattel, the California court in *Thrifty-Tel* noted that the requirement for a tangible intrusion in trespass has been attenuated so that the intrusion of microscopic particles, smoke, or dust can satisfy this element.⁵⁰ Indeed, in some cases, the migration of intangibles, such as sound waves, might constitute actionable trespass.⁵¹

I will resist the temptation to delve into a philosophical discourse about the comparative tangibility of electrons, microscopic particles, and the like, leaving the equivalence of matter and energy for physics textbooks. But I am less willing to concede the equivalence of trespass and trespass to chattels. The cases relied upon in *Thrifty-Tel* involve trespass to *land*, rather than trespass to *chattels*.⁵² The *Thrifty-Tel* opinion blithely glosses over this distinction, noting simply that both legal theories share a common ancestry. The *CompuServe* opinion also glibly intermingles trespass to chattels with doctrines related to real property. In doing so, these courts essentially reversed several hundred years of legal evolution, collapsing the separate doctrines of trespass to land and trespass to chattels back into their single common law progenitor, the action for trespass. But to do so effectively creates a brand new cause of action, unknown to modern jurisprudence.

Thus in the seminal *Thrifty-Tel* decision, the court not only substituted its own claim for a claim the plaintiff did not make, it was a claim the plaintiff could not have made, as the claim never existed before the court created it. Conflating these two types of trespass has serious consequences; they may share a common history, and even a common name, but they secure entirely different interests. Trespass to chattels exists as "the little brother of conversion."⁵³ The gravamen of both actions lies in the dispossession of the property from its owner. In conversion, the dispossession is total; in trespass to chattels, the dispossession is only partial. Neither entails the interest in inviolability that attends trespass to land. Indeed, even in the context of real property, impinging ephemeral substances such as smoke, or intangibles such as sound or light, typically have been addressed under doctrines of nuisance rather than doctrines of trespass. The "particulate trespass" cases relied upon in *Thrifty-Tel* were

⁴⁹ *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal Rptr. 2d 468, 473 n.6 (Cal. Ct. App. 1996).

⁵⁰ *Id.*

⁵¹ See *Wilson v. Interlake Steel Co.*, 649 P.2d 922 (Cal. 1982).

⁵² See, e.g., *Reynolds Metals Co. v. Martin*, 337 F.2d 780 (9th Cir. 1964); *Bradley v. American Smelting and Refining Co.* 709 P.2d 782 (Wash. 1985).

⁵³ See, e.g., *Reynolds Metals Co.*, 337 F.2d 780 (analyzing fluoride particulates); see generally W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 13, at 71 (5th ed. 1984).

largely cases in which the owner of real property had been dispossessed of the use of the land by contamination.⁵⁴

It is nearly impossible to recognize trespass to chattels in *Thrifty-Tel* or *CompuServe*, since the owners of the equipment were not in any way dispossessed of its use by the passage of electrons through the equipment in exactly the way the equipment was designed to carry them. Such "dispossession" by impinging electrons amounts to a rule of inviolability—the equipment was contacted by electrons, not touched, not damaged, not removed, not rendered inoperable. One wonders where the limits of such "trespass by electrons" might lie. If one is willing to base the physical contact requirement of trespass upon the receipt of electrons, then whole new vistas of electronic trespass are opened to our view. Unwanted telephone callers would seem to be engaging in trespass to chattels; the telephone call sends signals to the instrument of the recipient. So, too, with fax machines that receive unwelcome transmissions. Radios and televisions that receive unwanted transmissions are impinged upon by electromagnetic waves that induce the movement of electrons within the receiver.⁵⁵ I will not even begin to pursue here the endless possibilities for trespass upon household appliances plugged into electrical outlets, but instead leave such reflections to the reader's imagination.⁵⁶

B. Impairment

If the examples I have suggested sound a bit silly, that indicates the degree of regard properly paid to the "trespass" of electrons upon computers intentionally connected to a network designed to carry such electrons. The Restatement test guards against such trivial contacts by requiring that the contact rise to the level of some substantial interference equivalent to physical seizure of the chattel or similar deprivation of its use.⁵⁷ This may occur if the chattel is damaged or impaired as to its condition, quality, or value. But in the case of Cyber Promotions's

⁵⁴ *Thrifty-Tel*, 54 Cal. Rptr. 2d at 473 n.6.

⁵⁵ The proposition that electromagnetic transmissions may invade a property right in television receivers is not altogether unprecedented, although it has been characterized as a nuisance rather than a trespass. See *Page County Appliance Ctr., Inc. v. Honeywell, Inc.*, 347 N.W.2d 171 (Iowa 1984) (holding computer radiation from a travel agency that disrupted television reception in neighboring appliance store to be a nuisance). In my trespass scenario here, the interference occurs via transmission on an FCC licensed frequency. Given the federal assignment of spectrum, I leave for another day an analysis of the preemptive clash between the station owner's quasi-property right to a particular broadcast channel and the television or radio receiver owner's right to the possession and enjoyment of his chattel.

⁵⁶ Although I feel constrained to point out that electrical current is far less benign than network packets, so one can envision a situation in which a power surge physically damages an electrical appliance. This almost certainly would occur without the consent of the possessor, and so perhaps a theory of trespass to toasters is not entirely insane.

⁵⁷ See RESTATEMENT (SECOND) OF TORTS § 217 (1965).

"impinging electrons," as in my examples above, the physical contact with the equipment is, of course, too slight to constitute seizure or deprivation or to cause damage.

Undaunted by this common-sense requirement, the court in *CompuServe* simply bifurcated the requirements of physical contact and impairment, holding that any contact was sufficient—as I have said, creating a novel rule of inviolability—and that any proximately related "harm" or loss of "value" would satisfy the requirement for damage. Note that this move cuts trespass to chattels free from its moorings of dispossession or the equivalent, allowing the court free reign to hunt for "impairment." But even so, considerable ingenuity was required to find an impairment related to the passage of spam across the system. It is scarcely credible to think that if CompuServe were to put its equipment up for auction either the day before passage of Cyber Promotions's spam over the network, or the day after the spam, that there would be any diminution in its market price due to the intervening transmissions. Instead, the court found a diminution in value from the loss of computer processing cycles and the use of computer memory required to handle the bulk e-mail messages. No matter that the e-mail messages processed by the recipient systems were precisely the type of communications the equipment was meant to process—they were unwanted communications, and so the court reasoned that they impaired the equipment by displacing more desirable communications.

This analytical leap on behalf of CompuServe also nicely accommodates my examples above, as communications instruments that are physically contacted by various sorts of electrical signals will be similarly "impaired" by similarly processing the sort of signals that the particular device was intended to process. A telephone engaged by an unwanted call is thus impaired in value because it cannot receive other, more desirable calls while dedicated to the unwanted communication. Radios and televisions receiving unwanted programming are impaired in their value because they cannot receive more desirable communications when tuned to that channel. It may be that the "impairment" varies wildly among these media—for example, because telephone systems are channel-switched rather than packet switched, each call that is received entirely precludes any other communication from being received by that instrument.⁵⁸ A few hundred such communications, rather than tens or hundreds of thousands, would be enough to impede any other use of a telephone or fax machine. A radio or television receiver, on the other hand, can be severely impaired by a single signal on a particular frequency.⁵⁹ And unlike the very sensible Restatement requirement of damage to a physical chattel, impairment of this type is pretty much in the eye

⁵⁸ See Vinton G. Cerf, *Networks*, SCI. AM., Sept. 1991, at 72, 74; DANIEL P. DERN, *THE INTERNET GUIDE FOR NEW USERS* 6-8 (1994).

⁵⁹ See DERN, *supra* note 58, at 7.

of the beholder—the signal need not preclude any use of the device; it need only be unwanted.

As an alternative form of “impairment,” the *Hamidi* opinion finds damage in the loss of employee time occasioned by the spam.⁶⁰ This reasoning is, of course, absurd. The Restatement test clearly speaks in the first instance to the impairment of the *chattel*. It may be that Intel’s employees are less productive because of time wasted reading Hamidi’s communications, or that CompuServe’s technical staff is unprofitably employed trying to block Cyber Promotions’s spam, and that both companies lose money as a result. But employees are not chattels (at least not in the legal sense of the term). In each instance, the company’s computer system is the chattel whose impairment must be measured, and lost employee value is not an indicator of lost chattel value. In some instances, it might be sensible to measure the value of damage or impairment of a chattel by measuring the cost of labor to repair it,⁶¹ but that is not what the employees of Intel or CompuServe are doing in attempting to block unwanted messages. The trouble that the employees are addressing is not that the computer systems are functioning improperly, but rather that they *are* functioning properly, receiving transmitted bits precisely as they were designed and intended to do.

As a third alternative, the *CompuServe* court turned to the Restatement provision addressing the impairment of any legally protected interest when that impairment proximately flows from the interference with the chattel.⁶² It seems clear that what the Restatement criterion addresses is further *physical* harm proximately flowing from the initial harm to the chattel.⁶³ For example, emotional harm is not considered “harm” under this type of extended liability.⁶⁴ This is not to say that economic or dignitary harms are never actionable under trespass to chattels—we might consider, for example, the loss of business goodwill that could occur from delay of promised services if a business’s electronic files were damaged or locked.⁶⁵ CompuServe claimed similar loss of goodwill from disgruntled customers who complained or canceled their service when subjected to Cyber Promotions’s spam. But accepting this claim risks bootstrapping the interference with the chattel from the alleged harm to a protected

⁶⁰ Intel Corp. v. Hamidi, No. 98A505067, 1999 WL 450944 at *2 (Cal. Super. Ct. Apr. 28, 1999).

⁶¹ See, e.g., O’Brien Bros. v. The Helen B. Moran, 160 F.2d 502 (2d Cir. 1947) (discussing repair or replacement as alternative measures of damages).

⁶² CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997).

⁶³ See DOBBS, *supra* note 2, at 124-25.

⁶⁴ *Id.*

⁶⁵ Cf. State v. Moran, 784 P.2d 730, 732 (Ariz. Ct. App. 1989) (employee who refused to decode files criminally charged with “recklessly . . . tampering with the property of another person so as substantially to impair its function or value.”).

interest: loss of goodwill is only actionable if there is an interference, but we are told by the court that the interference lies in the loss of goodwill.⁶⁶

Additionally, it is not clear that the loss of subscription is sufficiently direct to be actionable: query whether, say, Federal Express can recover for loss of goodwill if a customer who receives objectionable mail via Federal Express—perhaps an unwanted demand letter from a creditor—thereafter chooses to boycott FedEx. It is not clear that CompuServe subscribers had a reasonable expectation that they would be shielded from a particular kind of network content. And let there be no mistake that in each of these cases the “harm” of the spam is unwanted content, and not some fictional lessening of goodwill or of the capacity of the proprietary network. If Hamidi had sent 30,000 messages to Intel employees telling them what an outstanding employer they work for, how fair and generous the company was to him in handling his workers’ compensation claim, and how they should get down on their knees each day and thank the gods for the privilege of working at Intel, presumably little would have been said in objection.

This “impairment by content” is even clearer in the case of CompuServe or AOL, which are, after all, businesses in the business of carrying bits. Subscribers to the system complained about the Cyber Promotions messages, but had Wallace offered them all something they were happy to see—say, certificates for free beer, or \$100 in e-cash—not a word would have been said. Indeed, were the system flooded each December with holiday greetings from every subscriber’s Aunt Maude or Uncle Albert, CompuServe presumably just would add more capacity—memory is cheap—and congratulate themselves on the popularity of their service. Thus, the “impairment” of the *chattel* amounted to no more than the receipt of annoying content, by which standard I must again conclude that my living room television is enormously impaired—indeed, the cable and broadcast networks have rendered it quite valueless.

C. Consent

The discussion above demonstrates that the finding of harm in these cases is dubious, at least a finding of harm that would make the passage of electrons over a computer system actionable as trespass. But there is of course no harm at all if the electronic “intermeddling” is privileged, as by consent.⁶⁷ The court in CompuServe found that some degree of tacit consent to e-mail transmissions could be inferred from the connection of the CompuServe system to the Internet.⁶⁸ CompuServe, Intel, and others

⁶⁶ In fairness to the Ohio court, it should be noted that this problem of circularity pervades the claim of trespass to chattels generally, and not merely the analysis in *CompuServe*. See DOBBS, *supra* note 2, fn.17 (noting that “The Restatement seems to attempt to fudge on this [extended liability] . . .”).

⁶⁷ See RESTATEMENT (SECOND) OF TORTS § 271 cmt. c. (1965)

⁶⁸ *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1023-24 (S.D. Ohio 1997).

whose machines are connected to the network have in some sense invited public usage of their equipment.

But the terms of such an invitation are murky. For example, it seems unlikely that by connecting to the network, CompuServe has opened its facilities to every conceivable use—for example, we would hardly infer that CompuServe's Internet connection constituted an invitation to commit computer crimes on its system, for example by "hacking" its servers to delete data, or to establish a free user account. Neither would it seem socially beneficial to impute to them some constructive invitation for such usage. At the same time, we might feel quite comfortable inferring from their connection to the Internet an invitation to transmit a variety of files, including personal e-mail, over their system. With regard to bulk e-mail, the question remains whether such usage lies within the terms of the invitation.

Our degree of comfort in inferring terms of assent rests to a large extent on what we believe may be the reasonable expectations of the parties. The law will generally gauge such by evaluating the backdrop of customary practices in the relevant community, considering the acceptable behaviors, or norms if you will, that the parties might have anticipated. But such norms change. At one time, no commercial traffic was acceptable on the Internet, in part because of an acceptable use policy promulgated by the sponsoring federal agency, the National Science Foundation, forbidding commercial traffic over its publicly-funded backbone.⁶⁹ The taboo against commercial use also stemmed in part from a deep-seated user understanding that bandwidth was scarce, and ought not to be wasted on irrelevant messages, or worse, on messages that seek private gain by free-riding on the digital commons. By the time of the first prominent case of commercial spam, by the infamous "green card" lawyers,⁷⁰ the Usenet community reacted with violent outrage because it was well understood that polite netizens simply did not act that way.⁷¹

The era of a non-commercial Internet is long since past, and commercial messages of every kind are now tolerated—even encouraged—on the net, or at least on certain portions of the net. Yet a particular bias against bulk e-mail clearly remains. Spam is of course annoying, but then so are banner ads and other advertisements in Internet media. If commerciality is the measure of offense, it is difficult to know what we should think about the case of Ken Hamidi, whose message was not commercial, at least not in the sense of proposing any transaction. Perhaps users accessing CompuServe should simply know that polite netizens do not send bulk e-mail, so that the attachment of their equipment to the network does not include a license for such usage. But if this is the reasonable expectation, then Hamidi's case is doubly vexing, since his version of

⁶⁹ See DERN, *supra* note 58, at 14.

⁷⁰ G. BURGESS ALLISON, *THE LAWYER'S GUIDE TO THE INTERNET* 40-41 (1995).

⁷¹ *Id.* at 42.

spam carried a social or political message about his former employer, intended for his former colleagues, to be read in the physical context where the message would have its maximum impact.⁷² If we were to make any inference about permission, it would likely be that Intel would decidedly *not* have agreed to such transmissions. Yet the Net seems generally to favor maverick messages, and Hamidi has in fact won cyberspace awards for challenging Intel. Does Hamidi violate Net norms by transmitting an acceptable message in a taboo vehicle?

Of course, in these particular cases, the question of inference may be something of a red herring. CompuServe and Intel sent letters to their respective e-mail nemeses, demanding that the spammers cease sending messages to addresses on the CompuServe or Intel networks. These letters were intended in part to give specific, explicit notice that the networks were not open to that particular use by Wallace or by Hamidi. By the time of trial, implied consent would not have been an issue. But then, it may be that the issue of consent is altogether a red herring. Couching the issue of access as one of consent frames the debate as a matter of contract, that is, a license to use property whose boundaries are already set. But as should be apparent by now, the *Thrifty-Tel* version of trespass follows the form of trespass to chattels, and yet has the substance of trespass to land. In that case, the question may be one of privilege rather than consent; that is, rather than a dispute over an agreement with one party, it might better be perceived as a dispute over the underlying right against the world. Property rights routinely are subject to public use; if a public easement lies across my land, it is open to public usage whether or not I have consented, no matter what kind of notice I post.⁷³ It may be that this new form of exclusory right should be subject to privileges that might allow offensive usage, such as politically charged bulk e-mail, whether or not the possessors would have agreed to such usage, and whether or not they gave explicit notice of their terms.

IV. TRESPASS IN CYBERSPACE

My goal to this point has been to show that the elements of common law trespass to chattels fit poorly in the context of cyberspace, and so the courts have been able to apply this claim to the problem of spam only by virtue of creative tailoring. Consequently, the cause of action masquerading in these cases as "trespass to chattels" is in fact a novel, hybrid form of a property right whose parameters have yet to be properly defined. Although this hybrid claim is novel, the incongruity of its elements with the operation of the Internet is not. The issues of tangibility, impairment, and consent that are discussed above appear as general problems in the

⁷² Intel Corp. v. Hamidi, No. 98A505067, 1999 WL 450944 at *1 (Cal. Super. Ct. Apr. 28, 1999).

⁷³ See ROGER A. CUNNINGHAM ET AL., *THE LAW OF PROPERTY* § 8.6, at 450 (2d ed. 1993).

law of proprietary control over digital media. The application of trespass is but the latest attempt to address these problems and raises the same concerns as previous attempts to subject Internet activity to a strict regime of exclusory rights.

A. *Copyright's Cousin*

To those who have followed the saga of intellectual property in the digital age, the machinations of courts attempting to fit trespass to the Internet will carry an eerie sense of déjà vu. Much the same set of legal gymnastics has been seen in judicial opinions attempting to fit copyright or patent to digital media. The fiction of impinging electrons is an excellent case in point. Despite their designations as "intellectual" property, patent and copyright in fact protect only the physical embodiments of innovation or creativity. In copyright, for example, the protected work must be fixed in a tangible medium of expression for more than a transitory time in order to qualify for legal protection.⁷⁴ Similarly, it is black letter patent law that patents do not protect disembodied ideas,⁷⁵ but rather their physical instantiation, and the Supreme Court made clear in the early 1980s that this rule applied to digital inventions like computer software.⁷⁶

But in digital media, the requirement of a tangible embodiment became distinctly problematic; the encoding of information as flux on magnetic media, or as voltages in silicon layers, seems relatively "tangible," but such embodiments may be highly transitory, or in some cases could disappear altogether when the current is turned off. In copyright, some courts have moved away from the requirement of stable, tangible copies and instead affirmed the copyrightability of ephemeral, so-called "RAM copies."⁷⁷ A similar progression has occurred in patent law, where the Supreme Court's requirement of physical embodiment for software has been systematically eroded by lower court decisions.⁷⁸ Much as in the case of copyrightable "RAM copies," such decisions find patentability on the theory that when software configures hardware, a new machine is cre-

⁷⁴ See MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.03[B], at 2-30.2 (1999).

⁷⁵ See DONALD S. CHISUM, CHISUM ON PATENTS § 101, at 1-5 to 1-6 (Dec. 1999).

⁷⁶ See *Diamond v. Diehr*, 450 U.S. 175 (1981); *Gottschalk v. Benson*, 409 U.S. 63 (1972); see generally Pamela Samuelson, *Benson Revisited: Patent Protection for Algorithms and Other Computer Program-Related Inventions*, 39 EMORY L.J. 1025 (1990).

⁷⁷ See, e.g., *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993) (holding program loaded into RAM was an infringing copy). But see *NLFC, Inc. v. Devcom Mid-America, Inc.*, 45 F.3d 231 (7th Cir. 1995) (holding terminals did not create statutory copies of programs in memory).

⁷⁸ See, e.g., *State Street Bank & Trust Co. v. Signature Fin. Group, Inc.*, 149 F.3d 1368, 1373 (Fed. Cir. 1998) (holding patentable "the transformation of data . . . by a machine . . . because it produces . . . a final share price momentarily fixed for recording and reporting purposes.")

ated.⁷⁹ Thus, under this theory, data structures in an otherwise conventional computer memory constitute a patentable invention.⁸⁰ Under the same theory, software encoded as sequences of flux on an ordinary floppy disc lend patentable novelty to the disc; after all, the configured disc is not the same article as an unconfigured disc.⁸¹

The parallel of these holdings to that of "electron trespass" is perhaps clearest in copyright, where the "RAM copying" cases find the transitory encoding of a work in computer memory is embodiment of a work under the copyright statute. This is of course a convenient fiction; the "copies" made in computer memories are in fact sequences of bits that configure the computer in such a way as to generate the work. The bits are not themselves a picture or poem, but rather instructions on how to recreate a picture or a poem. Protecting such arrangements of electrons or such sequences of magnetic flux does not seem too bizarre until one realizes that when such "copies" are moved around the Internet, no *copy* in fact moves, because the copyright statute defines copy as a "material object."⁸² In Internet transmission, the sender begins with a copy fixed in silicon or magnetic media, and a copy fixed in silicon or magnetic media appears at the point of receipt, but no material copy moves in between. Instead, instructions are sent from one server to another as to how to reproduce the work. This raises substantial doubt as to whether such digital transmissions can be counted as "distribution" for purposes of copyright, since under the statute, distribution requires transport of a tangible copy.⁸³

These problems have previously coalesced in the "linking" cases, where web site owners have objected to unauthorized hypertext links directed to their web pages.⁸⁴ A variety of legal theories have been raised against such links, but the most pertinent for illustrative purposes are the copyright claims against hypertext links. I have analyzed this question in detail elsewhere,⁸⁵ and so will only sketch the pertinent outlines of the problem here: the link itself is merely an address or reference to the page in question, and so it cannot constitute a direct copyright violation. Neither can it constitute contributory infringement unless some direct

⁷⁹ See, e.g., *In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994).

⁸⁰ See *In re Lowry*, 32 F.3d 1579 (Fed. Cir. 1994).

⁸¹ See *In re Beauregard*, 53 F.3d 1583, 1584 (Fed. Cir. 1995) (noting Patent Office concession that software residing on a floppy disc is patentable subject matter).

⁸² See 17 U.S.C. § 101 (1994).

⁸³ See Mark A. Lemley, *Dealing with Overlapping Copyrights on the Internet*, 22 U. DAYTON L. REV. 547, 556-57 (1997).

⁸⁴ See Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in Virtual World*, 82 MINN. L. REV. 609, 631 (1998).

⁸⁵ See Dan L. Burk, *Proprietary Rights in Hypertext Linkages*, 1998 J. INFO. L. & TECH. (June 30, 1998) <http://elj.warwick.ac.uk/jilt/intprop/98_2burk/>. For similar analyses, see Edward A. Cavazos & Coe F. Miles, *Copyright on the WWW: Linking and Liability*, 4 RICH J.L. & TECH 3 (Winter 1997) <<http://www.richmond.edu/~jolt/v4i2/cavazos.html>>; O'Rourke, *supra* note 84.

violation occurs. And where might the direct infringement be found? Only in the fleeting, intermediate copies that are made when the machine operated by a user of a link requests the material referenced by the link.

The trouble with this infringement analysis is of course that the owner of the material need not comply with the request to supply the referenced material. The fact that the owner's machine does so might be taken as implied consent to the intermediate reproduction, or may render the intermediate reproductions fair use in the course of an impliedly authorized use of the material.⁸⁶ And so the linking analysis turns upon a question of consent not unlike that in the trespass analysis above. The particular question in linking is whether by posting material to the network the owner has impliedly consented to transmissions that undoubtedly will occur and to the RAM copies that surely will be made whenever the material is accessed. The owner could, of course, restrict access to the posted material by requiring a password or by otherwise programming his server not to acquiesce to every request to download the copyrighted work. But copyright owners might equally well respond that the onus in the statute is not on them to secure their works against infringement; it is instead upon the public to refrain from unauthorized reproduction.⁸⁷

Indeed, as in the case of e-mail trespass, some content owners have attempted to rescind any implication of consent by posting notices on their web sites explicitly revoking consent to link to that site.⁸⁸ It is altogether unclear whether such a notice can be effective against the operator of a site that simply supplies the linking reference, or against someone who uses the link, since neither may have read the notice and the user, in fact, cannot have read the notice until after using the link such that the allegedly infringing copies are already made.

This problem of consent in network participation is not confined to the contexts of linking, copyright, and e-mail trespass; it appears to some extent as a generalized problem of online activity: whether we can and should infer from a certain course of conduct an intent to be bound by posted, but likely unread, contractual terms.⁸⁹ As I have suggested above,

⁸⁶ See Cavazos & Miles, *supra* note 85, at ¶ 54.

⁸⁷ See O'Rourke, *supra* note 84, at 659.

⁸⁸ See RESTATEMENT (SECOND) OF CONTRACTS § 21 (1979).

⁸⁹ Indeed, the question is general enough that the proposed Uniform Computer Information Transaction Act (UCITA), formerly known as draft U.C.C. Article 2B, contemplates making such an inference an adamant statutory condition. The literature concerning this presumption and related features of UCITA is extensive and highly polarized. For representative critical treatments, see, e.g., Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111 (1999); David Rice, *Digital Information as Property and Product: U.C.C. Article 2B*, 22 U. DAYTON L. REV. 621 (1997). For representative apologetics, see e.g., Lorin Brennan, *The Public Policy of Information Licensing*, 36 HOUS. L. REV. 61 (1999); Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13

we might draw inferences regarding the scope of contracts from custom and circumstance.⁹⁰ This standard attempts to take into account the expected behavior (or norms of conduct) surrounding the implied contract. However, it is notoriously difficult to determine the scope of implied contractual terms, and this may be particularly difficult where public behavior on the Internet is at issue. As recent commentary has pointed out, the Internet community now includes a diverse array of users with increasingly fewer shared expectations.⁹¹ Commercial messages such as "spam" are a case in point: at one time, commercial messages on the net were unthinkable; now they are relatively routine. It is probably safe to say that no one connecting to the network expects unauthorized intrusion or hacking. Similarly, it seems self-evident that anyone posting material to the Web should anticipate links to such material, but recent controversies over linking may be changing that expectation. The "reasonable" expectations for online use of copyrighted works may be difficult to assess because the activity is too new. And in the case of copyright, fair use may enable public use privileges different from those in traditional media. As in the case of bulk e-mail, the true issue for digital intellectual property may be less a matter of consent to the use of established property than of defining the scope of the property right itself.

B. *Trespass to Web Sites*

I suggest it is no accident that the problem of web linking recapitulates problems, such as the consent and content, found in the e-mail trespass cases. These problems are endemic to issues of ownership and control in digital media, and the application of trespass principles to bulk e-mail is an attempt to address the same issues that copyright has allowed to pass unsanctioned in web linking. In fact, Professor Hardy has suggested that the doctrine of trespass to land, rather than copyright, might better be applied to the issue of unauthorized hypertext linking.⁹²

BERKELEY TECH. L.J. 827 (1998); Robert Gomulkiewicz, *The License is the Product: Comments on the Promise of Article 2B for Software and Information Licensing*, 13 BERKELEY TECH. L.J. 891 (1998).

⁹⁰ See RESTATEMENT (SECOND) OF CONTRACTS § 65 (1998).

⁹¹ See Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998); see also Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J.L. & COM. 509, 516 (1996) (noting that "small close-knit . . . early cyberspace could govern itself as a commons but . . . later cyberspace probably cannot."); Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1309-10 (1998). Lemley and Radin level this critique at the assertion of David Johnson and David Post that the Internet should be largely, if not entirely, governed by the norms of net users. See David R. Johnson & David G. Post, *And How Shall the Net be Governed? A Meditation on the Relevant Virtues of Decentralized, Emergent Law*, in COORDINATING THE INTERNET 62 (Brian Kahin & James H. Keller eds., 1997).

⁹² See I. Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, 1996 J. ONLINE L. art. 7 <<http://www.wm.edu/law/publications/jol/hardy.html>>. But see Harold

Hardy's analysis sounds in trespass to land rather than trespass to chattels, but as I have suggested above, the trespass to chattels cases are in reality infused with a hefty dose of trespass to land.

Hardy's suggestion thus indicates that there is no particular reason the application of the *Thrifty-Tel* court's hybrid version of trespass need be limited to unwanted bulk e-mail. If the proprietary problem addressed by trespass is widespread in digital media, so too will be the elements necessary for the application of trespass, as found by the court in *CompuServe*. I have suggested above as an argument from absurdity that the elements of *Thrifty-Tel* trespass can be found in broadcast and telephony. But under the analysis in *CompuServe*, those elements are likely to be found in most online interactions, in which case the situation is not one of absurdity, but of frightening gravity.

Thus, taking a leaf from Professor Hardy's book, one might plausibly imagine that if trespass can be used to clear a system of spam, CompuServe or AOL could similarly clear their networks of undesirable Internet web content, such as transmissions from pornographic or white supremacist web sites. The elements of *Thrifty-Tel* trespass are clearly present in the case of unwanted web content. Electrons transmitted from web servers impinge on CompuServe's equipment, just as electrons do in the case of bulk e-mail. There is similarly a loss of data processing capacity in a recipient computer during use of the Web, as is will be apparent to anyone who has sat and waited for a web page to load. Indeed, so far as computer memory usage is concerned, the graphics-intense content of the World Wide Web is likely to occupy far more space than any typical e-mail message. Such web "trespass" is exacerbated by local caching of graphics files—in order to avoid repeated downloads of web graphics from the transmitting site, most browsers are programmed to "cache" such files on the viewers' hard drive.⁹³ This of course takes up memory far in excess of any given e-mail and perhaps even in excess of a fairly large bulk e-mailing.

But the diminution of value occasioned by web trespass does not stop with purloined processing cycles or commandeered disk sectors! As in the case of bulk e-mail, ISP employees may expend significant effort attempting to block transmissions from certain web sites.⁹⁴ ISP employee time may be consumed in installation of software filters designed to exclude

Smith Reeves, Comment, *Property in Cyberspace*, 63 U. CHI. L. REV. 761, 779-89 (1996) (arguing that cyberspace "property" interests should tend toward open boundaries).

⁹³ See I. Trotter Hardy, *Computer RAM "Copies": Hit or Myth? Historical Perspectives on Caching as a Microcosm of Current Copyright Concerns*, 22 U. DAYTON L. REV. 423, 426-27 (1997).

⁹⁴ See Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL'Y 475, 513 (1997).

pornographic, racist, or disparaging content.⁹⁵ Nonetheless, such sites may evade the filters by a variety of techniques, such as changing URLs, which requires ongoing ISP vigilance and software upgrades. Such content may also lower customer satisfaction by annoying or upsetting users of the system who do not wish to view such materials. Indeed, distraught ISP subscribers may well cancel their subscriptions in horror at some of the content that floods onto their computers from the Web.

And of course the creator of the web site undoubtedly knows or should know that the transmitted files will occupy memory and consume processing cycles on the recipient machine; indeed, we might well say that the web site operator intends this result, as it is the natural and probable consequence of placing materials on the Web. Moreover, one can only assume that, as in the case of spam trespass, were the ISP to place the web site on explicit notice that their content was unwelcome on the ISP's system, the web site operator could no longer plead ignorance or some implied license to transmit content to the ISP computers.

In light of the web linking discussion above, one might try to distinguish e-mail trespass from web trespass by claiming that e-mail is "pushed" or directed toward a recipient machine, whereas HTML files are "pulled" by request to the recipient machine.⁹⁶ Analytically, this amounts to a distinction in consent, on the basis that the download of the web-based content occurs in response to a request from the recipient's browser that the web site server transmit those files. But such an attempt to distinguish web transmissions from e-mail transmissions is illusory. Consider, for the sake of convenience, the transmission of derogatory web content from Hamidi's web site to an employee's work station at Intel after Intel has forbidden Hamidi to transmit web files to their system. Surely the situation is no different than a request from an Intel employee that Hamidi send a disparaging e-mail to him at work after Intel has demanded that Hamidi cease such e-mail transmissions. In either case, Hamidi is on explicit notice that his bits will be trespassing on Intel's machines, negating under the *CompuServe* analysis any consent that might be implied from Intel's connection to the net.

Web content transmission may also seem less directed and less intentional because web servers typically transmit the files automatically in response to a request for the files associated with a particular URL. But we must not be distracted by the degree of automation involved in transmitting files from the web site. The web site operator is unlikely to vet each request for access and manually enable the downloading of the requested files. But neither need the bulk e-mailer manually vet and transmit the spam sent from his machine; the process of collecting e-mail

⁹⁵ *Id.* See also Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453 (1997).

⁹⁶ See Timothy Wu, Essay, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1167 (1999).

addresses and spamming them may be entirely automated. In neither case is the individual responsible for the transmission likely to have actual knowledge of the URL to which the file is being sent; in either case the individual responsible could, in theory, know or discover the recipient's address.

Note that this application of trespass is quite the inverse of the sort of "web trespass" that Professor Hardy envisioned, by propertizing *recipient* machines rather than *transmitting* machines.⁹⁷ Where Hardy had hoped to use the doctrine to prevent unauthorized linkage—that is, file requests—to web sites, under the *CompuServe* analysis, this cause of action would deter unauthorized transmissions *from* web sites. Such a theory would effectively put the content provider in the position of having to screen requests for downloads, rather than putting the access provider in the current position of having to screen downloads requested from its system. And due to the peculiarities of consent, ISPs could, at their whim, trigger trespass claims by simply sending such sites letters informing them that their content is not welcome on their network, and that they should not transmit HTML or other files to addresses on the ISP's networks.

Lest anyone should think that such trespass claims would be limited to e-mail or the Web, similar analyses could easily be supplied for FTP, telnet, streaming audio or video, Internet "chat" sessions, software agents, indexing "spiders," and many other online applications. Trespass may indeed be the all-purpose cause of action for the Internet; the impingement of electrons and the "damage" of occupied memory is inherent in connecting a machine to the Internet, so the application of the claim is limited only by a plaintiff's imagination. Consider, for example, the recent dispute between the online auction site eBay and an auction aggregator service called AuctionWatch.⁹⁸ AuctionWatch offers a "Universal Search Function" that allows users to simultaneously access price, description, and bidding data from eBay and competitor services such as Amazon, Yahoo, and Lycos.⁹⁹ EBay objected, claiming that its auction data is proprietary, although the basis for this claim is unclear. Individual bits of data are not copyrightable, and it is uncertain whether eBay has exercised any copyrightable originality in the selection and arrangement of its bid information.¹⁰⁰ Nonetheless, eBay has threatened in its demand letter to AuctionWatch to explore all of its "legal, business, and engineering options."¹⁰¹

It takes little imagination to see that one of those legal "options" is an action for trespass to chattels under *CompuServe*, the elements of the

⁹⁷ See Hardy, *supra* note 92.

⁹⁸ See Troy Wolverton, *AuctionWatch Supplies eBay Listings Despite Block*, CNET NEWS (Jan. 18, 2000) <<http://news.cnet.com/news/0-1007-200-1525654.html>>.

⁹⁹ See *Auction Conflict Escalates*, WIRED NEWS (Oct. 11, 1999) <<http://www.wired.com/news/business/0,1367,31850,00.html>>.

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

claim are all present. Physical intrusion? Sometime during the search, electronic informational packets are undoubtedly exchanged between AuctionWatch and eBay, providing the requisite impinging electrons. Notice? One might infer that by placing its site on an open network and providing search capability, eBay has invited the public to search at will; but of course, since the receipt of eBay's demand letter, AuctionWatch is on explicit notice that its searches are unauthorized. Use? eBay naturally asserts that AuctionWatch's automated searching slows down eBay's service, burdening its servers¹⁰²—a factual claim that should sound familiar to anyone who has read this far. Moreover, eBay has taken the step of blocking requests from AuctionWatch¹⁰³—AuctionWatch has considered evading the filters by transmitting from alternate IP addresses¹⁰⁴—so eBay employee time has surely been consumed. The same analysis would be true if applied to Yahoo, Lycos, Amazon, and other sites searched by AuctionWatch. Of course, Yahoo and Lycos have built their core business around indexes generated by searching other web sites, so the same claim might be applied to them

In other words, the essential elements of *CompuServe* trespass are readily found in almost any online activity; the cause of action might better be named "using a networked computer." The Internet operates by allowing users to exchange electrons, consume processing cycles, and occupy disc space on its constituent machines. Following the path laid out in *CompuServe* and *Thrifty-Tel*, it is quite possible to torture the doctrine of trespass to chattels to cover any number of odious or inconvenient communications "like a nose of wax which may be turned and twisted in any direction"¹⁰⁵ Unfortunately, such contortions are not at all unlikely where Internet communications are at issue, and the process of expansion has likely already begun—all that any user needs to fulfill the elements of trespass is to withdraw consent for some real or imagined offense. Of course, as a friend of mine is fond of saying, there are no problems, only business opportunities: one begins to wonder if there may not be huge profits to be made in the creation of database software to allow future Internet users to keep track of the sites that have withdrawn their consent for this or that type of usage, with the novel threat of trespass to galvanize sales.

C. *Incomplete Entitlements*

The image of Internet users assiduously trying to avoid trespass suits by maintaining great databases of access authorization seems to me more than a little dystopic, but perhaps that is my particular bias; indeed, Prof.

¹⁰² See Troy Wolverton, *AuctionWatch Nips at eBay's Heels*, CNET NEWS (Oct. 5, 1999) <<http://news.cnet.com/news/0-1007-200-205529.html>>.

¹⁰³ See Craig Bicknell, *Auction Tiff: eBay Strikes Back*, WIRED NEWS (Nov. 4, 1999) <<http://www.wired.com/news/business/0,1367,32323,00.html>>.

¹⁰⁴ *Id.*

¹⁰⁵ *White v. Dunbar*, 119 U.S. 47, 51 (1886).

Hardy has implied that this is precisely the direction that network development should take, applying automation to enable a ubiquitous web of licensing negotiations with the owners of ever more finely-grained levels of network property.¹⁰⁶ My contrary view stems from the assumption that there are public benefits to be had in a cyberspace network that are not captured, and indeed may be destroyed by over-propertyization. In the spam cases, a version of this latter argument appears in an appeal to First Amendment doctrine. In the case of bulk e-mail, the courts rightly rejected such claims for lack of state action and similar doctrinal defects.¹⁰⁷ But even though the appeal to free speech may be misguided as a doctrinal matter, it need not be as a matter of policy. The issue of public access to communication naturally manifests itself as an appeal to the First Amendment, largely because the First Amendment exists to foster a particular type of public good: speech.¹⁰⁸ Thus the argument may be correct in its identification of public goods policy rather than in its appeal to the particular doctrine of free speech.

Setting aside the particular incarnation of the appeal for public access, the consideration of the right to exclude users from what generally is a shared communications resource raises a complex series of societal considerations. As part of its argument in *Hamidi*, Intel took the position that connecting its system to the Internet did not make its computers a "public" system.¹⁰⁹ In some senses this assertion is clearly true, even trivial. For example, Intel, not the public at large, continues to be responsible for the maintenance of its equipment. But at the same time, the act of joining a local network to the great "network of networks" that comprises the Internet indicates a desire to take advantage of the positive network externalities of the digital commons. Thus the consideration in granting a right to exclude is not so that Intel's system is "public" because it is open to the public, but because Intel itself derives benefit from the public nature of network.

Of course, public or common property has both its upside and its downside. The claim of trespass is to some extent an attempt to avoid a negative externality, that is, the cost imposed by spammers upon network users. Such impositions are facilitated in part by the public nature of the

¹⁰⁶ See I. Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI LEGAL F. 217; see also Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management of Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998). Prof. Cohen has offered an extended and devastating critique that challenges the foundations for this view. See Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of 'Rights Management'*, 97 MICH. L. REV. 462 (1998).

¹⁰⁷ See *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1025-27 (S.D. Ohio 1997); *Intel Corp. v. Hamidi*, No. 98A505067, 1999 WL 450944 at *2-3 (Cal. Super. Ct. Apr. 28, 1999). See also *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F. Supp. 436, 447 (E.D. Pa. 1996).

¹⁰⁸ See RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* 729-30 (5th ed. 1998) (discussing speech as a public good).

¹⁰⁹ *Hamidi*, 1999 WL 450944, at *2.

network. Spammers may use the digital commons at a marginal cost to them that approaches zero, and consequently, they do so without considering the external costs of their usage. It would clearly be desirable to force bulk e-mailers to internalize that cost, taking it into consideration in deciding how much e-mail to generate. Typically, external costs imposed upon a common resource may be internalized by creating private property interests that give users an incentive to consider the full cost of their usage, or seek permission to impose usage costs upon the property of another.¹¹⁰ Thus, propertizing the Net may initially seem an attractive way to accomplish this: by granting local system operators a right to exclude, they could force spammers to negotiate for a license, the cost of which presumably would reflect the cost of spam to the local operator.

However, propertization may itself impose costs on the use of the network, costs which ultimately could prove to outweigh the costs imposed by spam. The impetuous introduction of exclusive rights into the commons may lead to the situation that Michael Heller has dubbed the "anti-commons," in which property rights are so finely divided that it becomes essentially impossible to conduct any type of business.¹¹¹ In such highly fragmented property systems, myriad licenses must be obtained from the many, many owners before any type of large-scale project can be undertaken. The transaction costs involved in locating the rights holders and negotiating separate licenses with each of them will tend to deter complex endeavors. One can imagine the anti-commons nightmare that could ensue on the Internet in web linking, indexing, and other routine functions if every owner of equipment attached to the network were granted a cause of action for the trespass of unwanted electrons on her equipment.

As a related matter, introduction of private ownership rights into shared resources also will tend to lead to the classic "hold-out" problems that occur in real property whenever a large number of properties are involved in a project.¹¹² For example, the extended land corridors required for construction of a railroad or other public transportation system may impinge upon the properties of many owners. If rights of way must be negotiated from all the affected owners, any given owner may "hold out" for a price up to the full value of the project; after all, without that property owner's consent, there will be no project.¹¹³ If every property owner does this, and game theory suggests that each will have strong

¹¹⁰ See Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347-357 (1967).

¹¹¹ See Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998) (describing fragmented property rights in former communist nations); see also Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCI. 698 (1998) (arguing that fragmented property rights in gene sequences may create an anticommons).

¹¹² See Lloyd Cohen, *Holdouts and Free Riders*, 20 J. LEGAL STUD. 351 (1991).

¹¹³ *Id.*

incentive to do so, then the project becomes essentially impossible: the aggregate price demanded by the holdouts may exceed the value of the project.¹¹⁴

In the case of public works, society typically has solved the "anti-commons" and "hold-out" problems via powers of eminent domain and governmental takings: property owners' exclusive rights are simply negated in the public interest.¹¹⁵ In essence, their right to exclude is replaced with a right to compensation, substituting a liability rule for a property rule.¹¹⁶ Additionally, the imposition of a compulsory license on property holders is not limited to governmental takings; private actors may also be empowered to break an exclusionary "hold-out" logjam. For example, I have argued elsewhere that in the context of intellectual property, copyright doctrines including fair use and the idea/expression dichotomy allow private "takings" from copyrighted materials whenever intellectual "rights of way" are required in the creation of a new work.¹¹⁷ Alternatively, compulsory licensing systems may provide for such private "takings" of copyrighted works at a set royalty.¹¹⁸ Indeed, copyright fair use may be considered a type of compulsory license at a royalty of zero.¹¹⁹

This suggests that an unqualified exclusionary right in the form of trespass will tend to create in cyberspace at least the types of problems seen in real property. But the Internet may present additional problems not generally seen in real property, due to so-called "network effects." Network effects may arise in situations where the value of a system increases as users are added.¹²⁰ Purchasers of such goods find the good more valuable as others also purchase the good. Typically, the increased value accrues to subsequent adopters, and accrues as a positive externality.¹²¹ For example, a telephone system is of relatively little value if it has only two subscribers; each subscriber can call only one other person.¹²²

¹¹⁴ See Posner, *supra* note 108 at 62-63.

¹¹⁵ *Id.*

¹¹⁶ See *Ruckelshaus v. Monsanto Co.*, 467 U.S. 968, 1016-17 (1984); *Clouser v. Espy*, 42 F.3d 1522, 1539-40 (9th Cir. 1994) (holding that only damages are available for takings, not injunctive relief); see generally Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972) (distinguishing property rules and liability rules on the basis of the right to exclude).

¹¹⁷ See Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 140 (1999).

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ See Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424 (1985).

¹²¹ See S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. 133, 135 (1994) (distinguishing between positive and negative network effects).

¹²² See Katz & Shapiro, *supra* note 120, at 424 (citing telephones as an example of network effects); Liebowitz & Margolis, *supra* note 121, at 139-40 (noting the telephone system as a "paradigmatic" example of network effects).

The system is of greater value if it has more subscribers; each subscriber can call many others. Those who subscribe to the system after it has accrued a large number of subscribers may obtain a more valuable service than those who subscribed early, when there were few other subscribers. At the same time, the value of the service to the early subscribers grows as additional users sign on.

The Internet, not surprisingly, is a prime candidate for display of such network externalities: network access becomes more valuable as it becomes more ubiquitous.¹²³ Much of the success of the Internet itself is due to the creation of a new type of physical network: the inter-networking protocols on which the Internet operates allow disparate types of computer hardware, running many different software systems, to interact on a single network. Thus, users with previously incompatible equipment now can join the same system. Additionally, any given application run on the network may show a different kind of network effect from usage: e-mail, for example, is a more valuable service if it can be used more widely. Similarly, the World Wide Web becomes more valuable as it accumulates more reference linkages, allowing more information to be indexed and accessed.

Given these types of effects, it seems clear that divided ownership in a network will tend to exacerbate rather than solve any problem of external costs.¹²⁴ Under an exclusionary rule such as trespass, the imposition of myriad proprietary rights effectively fragments the network, allowing sites that have been physically connected to the network to segregate themselves legally from the network.¹²⁵ Stated differently, propertization in a networked environment encourages the holder of the exclusive right to attempt to free-ride upon the external benefits of the network, while at-will avoiding contribution of such benefits to others.¹²⁶ For example, in the *Hamidi* case, Intel apparently wished to enjoy the advantages of e-mail access to the Internet from its system, which was the reason it connected its machinery physically to the network. At the same time, it hoped to make its system unavailable to Hamidi, at least for the transmission of content that the company found objectionable. A similar calculus

¹²³ See Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 551 (1998).

¹²⁴ *Id.* at 560.

¹²⁵ See Lemley, *supra* note 91, at 1281.

¹²⁶ Both activities are simultaneously possible because the Internet exhibits more than one type of network effect, a point that may require some brief explanation. Katz & Shapiro have distinguished between actual and virtual networks. See Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 95 (1994). To the extent that the Internet generates benefits to users by their machines, physically connected to the network and allowing interaction between users, it represents an actual network, whereas the software or, for that matter, the content on the system does not. A legal trespass rule in large measure purports to exclude users from the benefits of the virtual network while allowing the site owner to remain connected to the actual network.

pertains in the case of eBay, which has profited from the easy and ubiquitous access to its auction service made possible by the open standards of the Internet. However, when the same open standards make possible added value generated by a service such as AuctionWatch, eBay suddenly opposes open access—unless of course it can capture that value.

In each of these cases, a particular use of the local system may be locally objectionable but globally beneficial, as is arguable in the case for Hamidi's social commentary or AuctionWatch's aggregate search service. Intel or eBay may hope to avoid the local burden of networking by legal exclusion, but this eventually will result in suppression of the positive externalities of networking. This is a common theme in Internet governance, which I have dealt with at some length in other contexts.¹²⁷ Note, for example, that the tendency of companies like Intel or eBay to want to "secede" from the network is closely akin to the situation faced by the states in a federal system, where each polity would like to enjoy the benefits of federalism, while avoiding the local costs.¹²⁸ The United States has developed constitutional doctrines that ameliorate such behavior, notably the Dormant Commerce Clause, and I have analyzed elsewhere the constitutional ramifications of states' desire to virtually secede from the Internet.¹²⁹ Nations may behave similarly in the face of global networking, hoping to close their borders to the shared network costs while also hoping to garner shared network benefits.¹³⁰

Thus, the trespass rationale of *CompuServe* is simply border-drawing at the level of an individual system rather than at the level of a political entity.¹³¹ But as I have argued elsewhere, such attempts to draw borders in cyberspace walk a delicate line between internalizing negative external costs and negating the positive external benefits of the network.¹³² If propertization via trespass imposes costs in excess of the costs imposed by spam, it is difficult to justify recognition of trespass claims: they may do more harm to the digital commons than do the unauthorized uses they are designed to prevent. However, this comparison of harms may vary dramatically with circumstance. The degree of harm inflicted by spam or other unauthorized trespass may vary with the scope and the degree of intrusion. Some bulk e-mail, such as Hamidi's, may bear social messages of the type that might otherwise be protected by the First Amendment; other bulk e-mail may propose questionable "get rich" schemes of little social value. An optimal regulatory standard, rather than imposing a blanket possessory exclusion, might provide for consideration of comparative

¹²⁷ See Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095 (1996).

¹²⁸ *Id.* at 1103-07.

¹²⁹ *Id.* at 1133-34.

¹³⁰ See Dan L. Burk, *Virtual Exit in the Global Information Economy*, 73 CHI.-KENT L. REV. 943 (1999).

¹³¹ Cf. Reeves, *supra* note 92, at 762-67.

¹³² See Burk, *supra* note 130, at 970-71.

harm, imposing liability where the harm from the use exceeded that attending exclusion.

The need to balance social costs and benefits in this fashion suggests that the imposition of theories, such as trespass upon the digital commons, may tend to lead to detrimental over-propertyization of the Internet. Incomplete entitlements, rather than strong exclusive rights, might better serve the balancing function. I have argued elsewhere that such flexible or "muddy" entitlements may better accommodate diffuse societal values that would not be internalized by bright-line property rules.¹³³ Economic theory indicates that in situations where the costs of locating, negotiating, and valuing transactions are high, unclear entitlements may tend to facilitate bargaining.¹³⁴ Unclear rules will tend to facilitate innovative or informal bargaining arrangements, whereas bright-line rules appropriate to low transaction cost situations may simply lock the parties into their respective ownership positions, unable to reach a beneficial exchange.¹³⁵ Alternatively, the unclear rule may shunt disputes into third-party review, as in litigation, where the court can tailor an ownership rule to the specific situation.¹³⁶

These characteristics suggest that the correct property theory might be *nuisance* to web sites, rather than trespass. Nuisance lies only if the cost of the intrusive activity outweighs the benefit.¹³⁷ The "muddy" nature of nuisance would allow computer owners on the Net to exclude unreasonably costly uses of their servers, while allowing access for socially beneficial uses, even if the server owner might otherwise object. Stated differently, nuisance would authorize computer owners to legally "defect" from the network when necessary to avoid wasteful negative network externalities, but require them to remain legally networked when necessary to generate beneficial positive network externalities. Of course, the server owner always would have the option of physically disconnecting from the network to avoid objectionable uses, so long as he was willing to forgo the positive benefits of the network as well. Presumably, proper application of the nuisance standard would make this drastic action unattractive on average to rational server owners, as they would be shielded from marginally detrimental uses, while enjoying marginally beneficial network advantages.

Of course, the law of nuisance applies to real property, not to chattels. But this property distinction has proven no obstacle to courts thus far; as I have shown above, the current action called "trespass to chattels"

¹³³ See Burk, *supra* note 117.

¹³⁴ See Thomas W. Merrill, *Trespass, Nuisance, and the Costs of Determining Property Rights*, 14 J. LEGAL STUD. 13 (1985); see also Carol M. Rose, *Crystals and Mud in Property Law*, 40 STAN. L. REV. 577 (1988).

¹³⁵ See James E. Krier & Stewart J. Schwab, *Property Rules and Liability Rules: The Cathedral in Another Light*, 70 N.Y.U. L. REV. 440, 446 (1995); Merrill, *supra* note 134.

¹³⁶ See Burk, *supra* note 117, at 138.

¹³⁷ See Merrill, *supra* note 134.

in fact contains a healthy dose of jurisprudence from trespass to land. A form of cyberspace nuisance claim, containing a healthy dose of real property doctrine, might better accommodate the peculiar calculus of benefits and harms in cyberspace.

V. CONCLUSION

Let me conclude by observing again that I find spam to be just as bothersome as anyone else does, and the actual result of cases like *CompuServe v. Cyber Promotions* to be salutary. Even the argument that bulk e-mail constitutes trespass to chattels is an admirably clever bit of lawyering, effective in securing a desired benefit to Internet service providers in the short-term. But the long-term effects of the trespass theory are likely to be pernicious, and the disturbing implications of the *Hamidi* case signal the first movement toward a pathological division of the digital commons. Widespread application of this new form of hybrid trespass would negate the benefits of shared resources on the network. Indeed, the logical endpoint of such a trespass theory may be a sort of "anti-commons" in which the rights of use on the net are so fragmented as to prevent anyone from accomplishing anything useful.

This is not to say that some remedy against abuse of local networks ought not be provided, only that it ought not to blossom into a generalized form of intangible property right. The trick is to deter only those "abuses" that outweigh global benefits. One approach to accomplishing this task may be to penalize abuse via statutes designed specifically to deter unauthorized access; as I have suggested above, any consent to system usage that might be implied from connection to the Internet surely does not include "hacker" intrusion—but statutes can be written to target such clear abuses.¹³⁸ To the extent that we wish to deter spam as an abuse, it might be analogized to abuse in previous media, such as repeated unsolicited telephone calls, that would constitute some form of harassment. Repeated unsolicited telephone calls, or repeated unsolicited faxes have been addressed directly by statute.¹³⁹ Similar legislation for bulk unsolicited e-mail may be the preferable response to the problem of "spam" so long as the statute comports with the requirements of the First Amendment.¹⁴⁰ This type of narrowly tailored legislation prevents a sort of legal "mission creep" that allows a common law doctrine to

¹³⁸ See generally, Alois Valerian Gross, Annotation, *Criminal Liability for Theft of, Interference With, or Unauthorized Use of Computer Programs, Files, or Systems*, 51 A.L.R. 4th 971 (1987).

¹³⁹ See, e.g., 47 U.S.C. § 227(b)(1)(C) (1994) (prohibiting faxed advertisements).

¹⁴⁰ See *ACLU v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997) (invalidating Georgia fraudulent transmissions statute on First Amendment grounds); Jennifer M. Kappel, Comment, *Government Intervention on the Internet: Should the Federal Trade Commission Regulate Unsolicited E-mail Advertising?*, 51 ADMIN. L. REV. 1011, 1028 (1999) (stating that legislation aimed at spam must balance the public's interest in being free from false advertising while not infringing on the First Amendment).

mutate from the cure for an isolated problem to the pathology in a broad body of caselaw.

At the same time, statutory fixes may be too narrow, leading to a proliferation of legal code.¹⁴¹ Because flexibility and adaptability to new situations is one of the virtues of the common law system, it may be worth exploring which other common law doctrines might alternatively be impressed into service to deter the unwanted activity without balkanizing the network. I have already suggested above that a cyberspace version of private nuisance might serve such ends, there may be other common law doctrines that would serve as well.¹⁴² For example, restitutionary claims such as unjust enrichment or accounting for profits have been used in real space to deter unauthorized uses of another's chattel.¹⁴³ A common law theory of this type may be less likely to tend toward exclusionary rights; although judicial opinions in such cases pay homage to the exclusionary right of property holders,¹⁴⁴ they do not confer a right to exclude, only a right to recover.¹⁴⁵ Because the recovery is premised upon the monetary benefit gained by the wrongdoer rather than upon the damage to the plaintiff, this approach may be an appropriate deterrent where a defendant—such as a spammer—has profited, but no credible damage has occurred. This characteristic of the claim may tend to deter unauthorized uses, rather than forcing Hamidi's non-commercial messaging into the same box as the Cyber Promotions spam.

But even here some care must be taken that "unjust" enrichment designates profits accrued by imposing negative local costs in excess of the global benefit. If there is a baseline expectation that all "use" of a networked system must be authorized, and perhaps paid for, then any transmission becomes automatically transformed into an "unjust" enrichment, and this claim, too, would simply denominate a type of systems

¹⁴¹ I leave for another day the consideration of solutions based on computer code. See generally LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

¹⁴² For suggestions along these lines, see Anne E. Hawley, Comment, *Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 UMKC L. REV. 381 (1997).

¹⁴³ See, e.g., *Olwell v. Nye & Nissen Co.*, 173 P.2d 652 (Wash. 1946) (requiring defendant to pay for unauthorized use of plaintiff's egg-washing machine). This theory apparently has been asserted in one or two successful actions against bulk e-mailers. See Hawley, *supra* note 142, at 421-22 (detailing unpublished injunction orders). Unfortunately, it is trespass to chattels rather than unjust enrichment that has taken center stage in published opinions.

¹⁴⁴ See *Olwell*, 173 P.2d at 654 ("The very essence of the nature of property is the right to its exclusive use.").

¹⁴⁵ See Douglas Laycock, *The Scope and Significance of Restitution*, 67 TEX. L. REV. 1277, 1283 (1989) (distinguishing restitutionary from injunctive relief). Note that trespass to chattels is "restitutionary" in that it restores something taken, but does so in tort rather than as a matter of unjust enrichment. See RESTATEMENT OF RESTITUTION ch. 7 introductory note at 523 (1937).

trespass. Instead, what is required are carefully calibrated causes of action sounding in restitution or in "hybrid" nuisance to provide the proper incentives against network abuse without worsening the trouble with trespass.¹⁴⁶

¹⁴⁶ Unjust enrichment might be valuable in deterring commercial spam by enabling a remedial choice as to whether the proper measure of damages would be the profit the unauthorized user made from the use or the value the owner might have gotten from his preferred use. In a case such as *Ohwell*, it may be that the restitutionary remedy is simply a punitive remedy imposed on the unauthorized commercial user for failure to bargain for permission to use the chattel. *See generally* DOUGLAS LAYCOCK, MODERN AMERICAN REMEDIES 531, 533 (2d ed. 1994). In the case of bulk e-mail, the true harm may be the failure of Cyber Promotions to bargain for access to CompuServe's system, as that would allow both actors to internalize the costs associated with commercial e-mail broadcasts to subscribers.